Księga procedur

ZATWIERDZAM

BURMISTRZ

mgr Piotr Ćwikła

.....

podpis Burmistrza

METRYKA

Nazwa jednostki	Urząd Miejski w Łobzie		
Tytuł dokumentu	Księga Procedur		
Opis	W skład dokumentu wchodzą: Księga procedur wraz z załącznikami		
Zastosowanie	Urząd Miejski w Łobzie		
Plik	Księga procedur		
Status	Dokument zatwierdzony, obowiązujący do stosowania od ..... 2018 r.	Liczba stron	16

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	20.09.2018	utworzenie	wszystkie	Krzysztof Rychel	
2.00	15.10.2018	modyfikacja	wszystkie	Krzysztof Rychel	

* Np.: utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Procedura realizacji obowiązku informacyjnego. 4

2. Procedura nadawania i odbierania uprawnień 8

2.1 Nadanie upoważnienia 8

2.2 Odebranie upoważnienia 11

3. Procedura reakcji na ujawnione naruszenie 12

4. Procedura udostępniania danych osobowych 16

Załączniki: 17

1. Procedura realizacji obowiązku informacyjnego.

Prawo do wiedzy o tym, co się dzieje z danymi osobowymi jest jednym z podstawowych praw właściciela danych osobowych. Obowiązek informowania właściciela danych osobowych występuje w czterech podstawowych sytuacjach:

a) jeżeli dane są zbierane bezpośrednio od osoby (art. 13 RODO);
b) gdy dane osobowe są zbierane z innego źródła niż właściciel danych (art. 14 RODO);
c) zmieniając cel przetwarzania lub dodając nowy (art. 13 ust. 3 i art. 14 ust. 4 RODO);
d) w wykonaniu żądania dostępu do danych.

Wszystkie ww. sytuacje mogą wystąpić w następujących okolicznościach:

a) wpływ pisma do jednostki,
b) przekazanie pisma, sprawy przez inną komórkę w ramach jednostki,
c) bezpośrednia wizyta petenta w jednostce i rozpoczęcie sprawy na jego wniosek,
d) rozpoczęcie procedowania sprawy „z urzędu".

Postępowanie:

1. Rozpoczęcie przetwarzania danych osobowych może być efektem sytuacji wymienionych w pkt. od a) do d).

2. W momencie bezpośredniej wizyty petenta i zainicjowania sprawy, istnieje możliwość natychmiastowego spełnienia obowiązku informacyjnego lub w przypadku, kiedy nie jesteśmy do tego przygotowani ustalenia z nim sposobu jego spełnienia w najbliższej przyszłości.

3. W przypadku innym niż bezpośrednia wizyta petenta należy ustalić, czy wobec niego został spełniony obowiązek informacyjny np. przez stanowisko merytoryczne przekazujące nam jego sprawę. Uwaga! Za stanowisko merytoryczne nie uważa się stanowiska odpowiadającego za obsługę procesu przyjmowania korespondencji w jednostce (kancelaria, biuro podawcze, sekretariat). Za pierwsze stanowisko merytoryczne zobowiązane do spełnienia obowiązku informacyjnego uznaje się stanowisko wszczynające postępowanie w sprawie, niezależnie od sposobu jej realizacji. Jeżeli przedmiotowy obowiązek informacyjny został spełniony przez stanowisko rozpoczynające procedowanie sprawy, a my jedynie ją kontynuujemy, jedynym obowiązkiem jest zweryfikowanie czy czynność przetwarzania danych osobowych w związku z rozpoczętymi działaniami znajduje swoje odzwierciedlenie w *Rejestrze czynności przetwarzania danych osobowych* lub w *Rejestrze kategorii czynności przetwarzania,* które są przypisane do naszego stanowiska.

4. Jeżeli obowiązek informacyjny wobec petenta nie został spełniony przez stanowisko wcześniej procedujące w tej sprawie lub nasze stanowisko jest rozpoczynającym załatwianie sprawy, należy zweryfikować, czy czynności przetwarzania związane z podejmowanymi działaniami są ujęte w rejestrach, o których mowa w pkt. 3, przypisanych do naszego stanowiska. Jeżeli czynności przetwarzania danych osobowych, jakie będą realizowane przy procedowaniu sprawy, nie zostały ujęte w rejestrach, o których mowa w pkt. 3, to w pierwszej kolejności należy poinformować przełożonego, który winien uzupełnić zapisy stosownego rejestru o nowo zdefiniowane czynności przetwarzania danych, w szczególności definiując wobec nich: cel przetwarzania, podstawę prawną przetwarzania, okres przechowywania dokumentacji, wykaz odbiorców danych, a

następnie uzupełnić właściwy rejestr o zdefiniowane informacje. Szczegółowe elementy przedmiotowego rejestru określa załącznik nr 2 do *Polityki ochrony danych osobowych*.

5. Jeżeli czynności przetwarzania danych osobowych, jakie będą realizowane w związku z procedowaniem sprawy są ujęte w jednym z dwóch rejestrów, o których mowa w pkt. 3, to na podstawie zawartych w nich zapisów można przystąpić do przygotowania informacji, w wariancie uzależnionym od osoby przekazującej dane. W przypadku, kiedy procedowanie sprawy jest wynikiem inicjatywy osoby przekazującej własne dane stosowany jest wzór informacji z art. 13 RODO, natomiast jeżeli inicjatorem procedowania sprawy nie jest petent, lecz inny podmiot, zastosowanie ma wzór informacji dla właściciela danych z art. 14 RODO. Uwaga w przypadku, kiedy petent w związku ze sprawą wskazuje inne strony postępowania lub na skutek procedowania sprawy, sami ujawnimy strony postępowania, to wobec tak ujawnionych osób fizycznych, będących stronami postępowania, również istnieje konieczność spełnienia obowiązku informacyjnego przy zastosowaniu wzoru informacji z art. 14 RODO. Wzory wymienionych informacji z art. 13 oraz art. 14 RODO stanowią załącznik nr 4 do *Polityki ochrony danych osobowych*.

6. Kolejny krokiem postępowania jest ustalenie czy osoba, wobec której istnieje obowiązek informacyjny (wynikający z art.13, bądź 14 RODO), będzie w związku z procedowaną sprawą miała z nami kontakt osobisty, czy też nie. W przypadku założenia, że będzie istniała możliwość kontaktu osobistego (petent w związku ze sprawą pojawi się w jednostce), obowiązek informacyjny może zostać spełniony w dowolnej formie w trakcie wizyty petenta w związku ze sprawą. W przypadku, kiedy nie ma takiej możliwości lub przewidujemy, że petent nie pojawi się w związku z procedowaną sprawą, obowiązek informacyjny realizujemy w formie załączenia odpowiedniego wzoru do pierwszej korespondencji skierowanej do petenta. Uwaga niezależnie od przewidywań czas, jaki ustala się na spełnienie obowiązku informacyjnego wynosi 30 dni kalendarzowych, liczonych od daty rozpoczęcia procesu załatwiania sprawy (wpływu, złożenia wniosku, podania, prośby). Jeżeli więc przewidywany pierwszy kontakt z petentem (bezpośredni, bądź korespondencyjny) wystąpi po upływie wskazanego 30 dniowego okresu, jesteśmy zobowiązani do przyjęcia innej formy spełnienia obowiązku informacyjnego np. wysyłając informację o przetwarzaniu danych osobowych na adres petenta, jeżeli takowy jest w naszym posiadaniu.

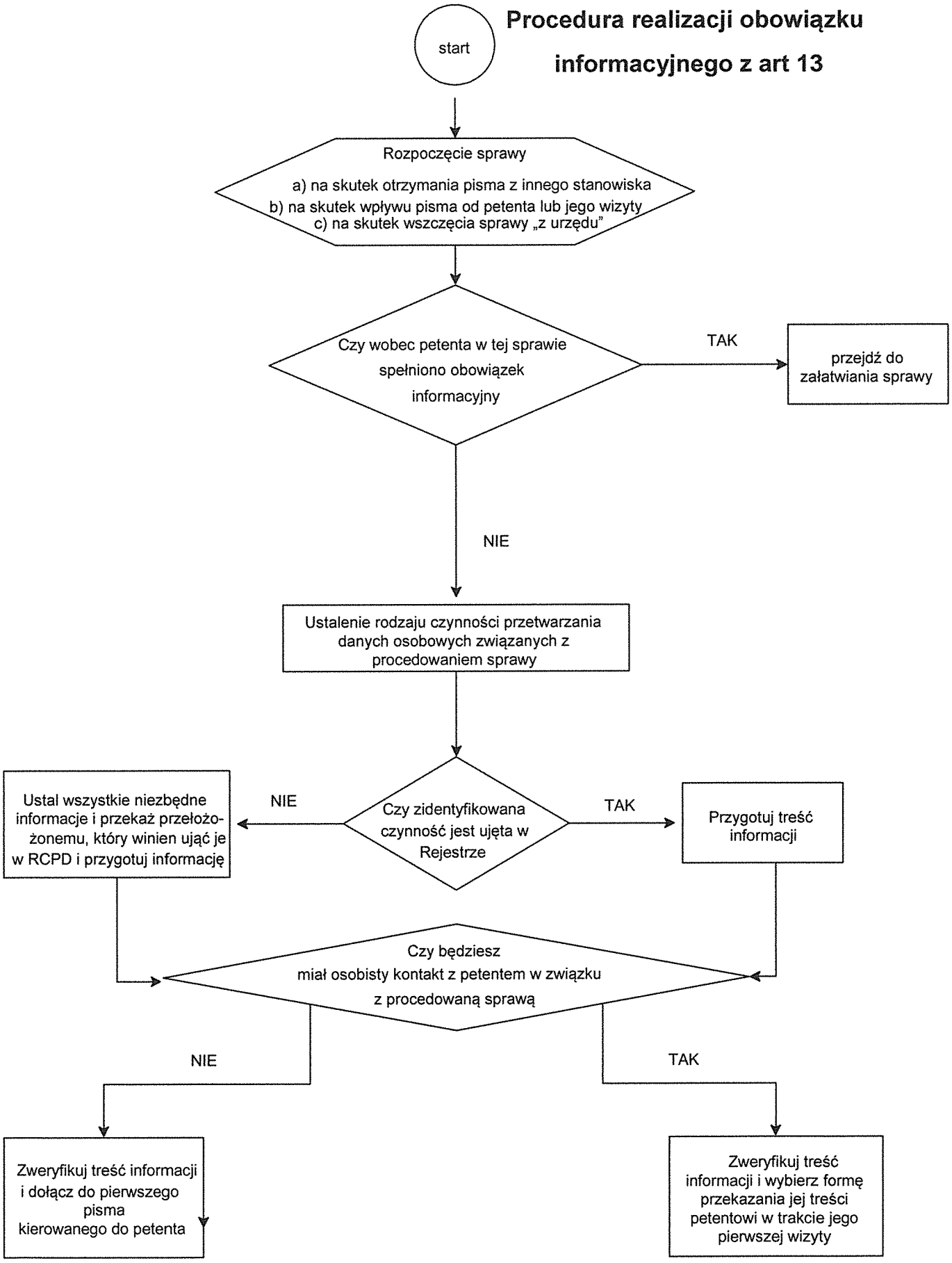
7. Powyższa procedura nie ma zastosowania w następujących sytuacjach:

   a) jeżeli treść informacji o sposobie przetwarzania danych stanowi integralną część umowy, wniosku, pisma wg wzoru opracowanego przez jednostkę, czy też decyzji, która zostanie wydana przed upływem 30 dniowego okresu, o którym mowa w pkt. 6,

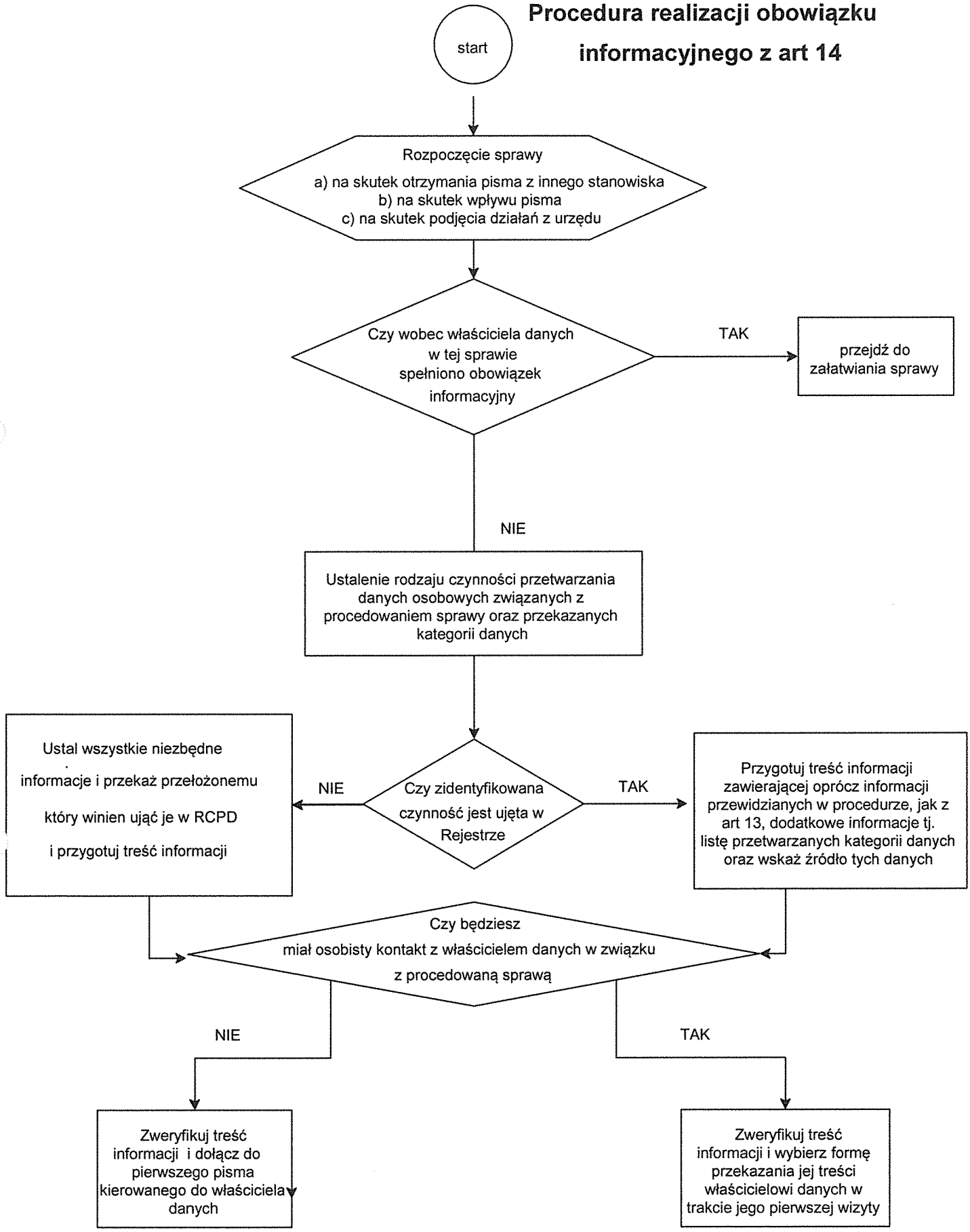
   b) jeżeli dane osobowe są przetwarzane w oparciu o zgodę ich właściciela, stanowiącą **załącznik nr 1** do niniejszego dokumentu, która zawiera w swojej treści wszystkie elementy informacyjne dla właściciela danych osobowych, określone w art. 13 RODO.

Przebieg procesów spełnienia obowiązku informacyjnego w formie graficznej zaprezentowano poniżej.

Procedura realizacji obowiązku informacyjnego z art 13



Procedura realizacji obowiązku informacyjnego z art 14



2. Procedura nadawania i odbierania uprawnień

2.1 Nadanie upoważnienia

Od każdej osoby zatrudnionej w jednostce, niezależnie od formy zatrudnienia, przed przystąpieniem do realizacji czynności przetwarzania danych osobowych wymagane jest posiadanie właściwego upoważnienia, umocowującego tą osobę do ich przetwarzania w sposób zgodny z zasadami określonymi w RODO i *Polityce ochrony danych osobowych*.

Obowiązek nadania właściwych uprawnień (upoważnienia) do przetwarzania danych osobowych może wystąpić w następujących sytuacjach:

a) zatrudnienie przez jednostkę nowej osoby w oparciu o umowę o pracę lub umowę cywilną,

b) zmiana miejsca zatrudnienia (komórki), niezależnie od przyczyny zmiany,

c) zmiana zakresu powierzonych obowiązków niezależnie od przyczyny zmiany (np. zastępowanie innych pracowników)

Postępowanie:

1. Upoważnienie jest wydawane przez administratora danych osobowych (ADO) lub osobę przez niego upoważnionej do nadawania upoważnień. Funkcję ADO definiuje i wskazuje *Polityka ochrony danych osobowych*, która również w załączniku nr 5 określa wzór wniosku o nadanie upoważnienia.

2. Wniosek o nadanie upoważnienia (wg załącznika nr 5 do Polityki ochrony danych osobowych) jest sporządzane przez samodzielne stanowisko ds. kadr w 3 egzemplarzach.

3. W przypadku przygotowania upoważnienia należy kierować się tzw. „zasadą wiedzy koniecznej", co oznacza, że pracownik może zostać upoważniony do czynności przetwarzania danych osobowych w zakresie wynikającym z powierzonego indywidualnego zakresu czynności, który to winien również zawierać czynności wynikające z przyjętego w jednostce systemu zastępstw.

4. Pierwszym krokiem w przygotowaniu wniosku jest konfrontacja czynności przetwarzania danych osobowych, jakie będą przedmiotem upoważnienia z zakresem obowiązków osoby upoważnianej oraz zweryfikowanie czy czynności z zakresu powierzonych obowiązków znajdują odzwierciedlenie w *Rejestrze czynności przetwarzania danych osobowych* (RCPD) prowadzonym w jednostce/komórce/na stanowisku pracy.

5. W jednym wniosku można nadać upoważnienie (w zależności od potrzeb), do kilku czynności przetwarzania danych osobowych, określając je w treści upoważnienia nazwą pod jaką występują w rejestrze, o którym mowa w pkt. 4 lub w przypadku większej ich liczby, posługując się numerami, za którymi występują w przedmiotowym rejestrze.

6. Wypełniony wniosek w 3 egzemplarzach jest przekazywany ADO lub osobie przez niego upoważnionej. Ze względu na możliwość nieobecności spowodowanej urlopem, chorobą, za zasadne należy uznać rekomendowanie rozwiązania, polegającego na pisemnym umocowaniu

odpowiedniej w hierarchii stanowisk, osoby do czynności związanych z nadawaniem upoważnień w imieniu ADO.

7. Po zatwierdzeniu przez ADO lub umocowaną przez niego osobę upoważnienia, formularz należy przekazać osobie pełniącej funkcję administratora systemu informatycznego (ASI). Funkcję ASI definiuje *Polityka ochrony danych osobowych*.

8. Zadaniem ASI jest weryfikacja czynności przetwarzania danych osobowych dla realizacji, których będzie wykorzystywany określony system informatyczny. W przypadku pojawienia się sytuacji związanej z koniecznością wykorzystania określonych systemów informatycznych, ASI dla każdego z nich, określa indywidualny i niepowtarzalny login dla upoważnionego.

9. ASI po nadaniu loginu/loginów, dokonuje jego/ich zapisu w treści wniosku o nadanie upoważnienia przekazuje wszystkie 3 egzemplarze do samodzielnego stanowiska ds. kadr. Ponadto ASI po wypełnieniu wniosku instruuje użytkownika odnośnie pierwszego uruchomienia systemu/systemów i zasad ich funkcjonowania, a następnie dokonuje właściwej konfiguracji jednostki komputerowej przypisanej do stanowiska pracy upoważnionego, w sposób zgodny z zasadami określonymi w *Polityce ochrony danych osobowych.* ASI dokonuje zapisów przydzielonych loginów w prowadzonym rejestrze stanowiącym załącznik nr 1 do *Instrukcji zarządzania systemem informatycznym*.

10. Samodzielne stanowisko ds. kadr odnotowuje nadane upoważnienie w Rejestrze stanowiącym załącznik nr 7 do Polityki ochrony danych osobowych i przekazuje użytkownikowi wszystkie 3egzemplarze do podpisu. Użytkownik po zapoznaniu się z przyjętą w jednostce dokumentacją określającą zasady funkcjonowania obszaru danych osobowych oraz treścią pouczenia zawartego w upoważnieniu, składa swój podpis pod treścią zamieszczonego we wniosku oświadczenia, zachowując jeden egzemplarz wniosku dla siebie. Kolejny egzemplarz samodzielne stanowisko ds. kadr przekazuje bezpośredniemu przełożonemu użytkownika, a trzeci archiwizuje na swoim stanowisku pracy, jako element prowadzonego Rejestru wydanych i odwołanych upoważnień.

11. Okres archiwizacji wydanych upoważnień jest określony okresem realizacji czynności przetwarzania danych osobowych, będących przedmiotem upoważnienia, powiększonym o okres kolejnych 10 lat po okresie zakończenia określonych czynności przetwarzania na stanowisku pracy.

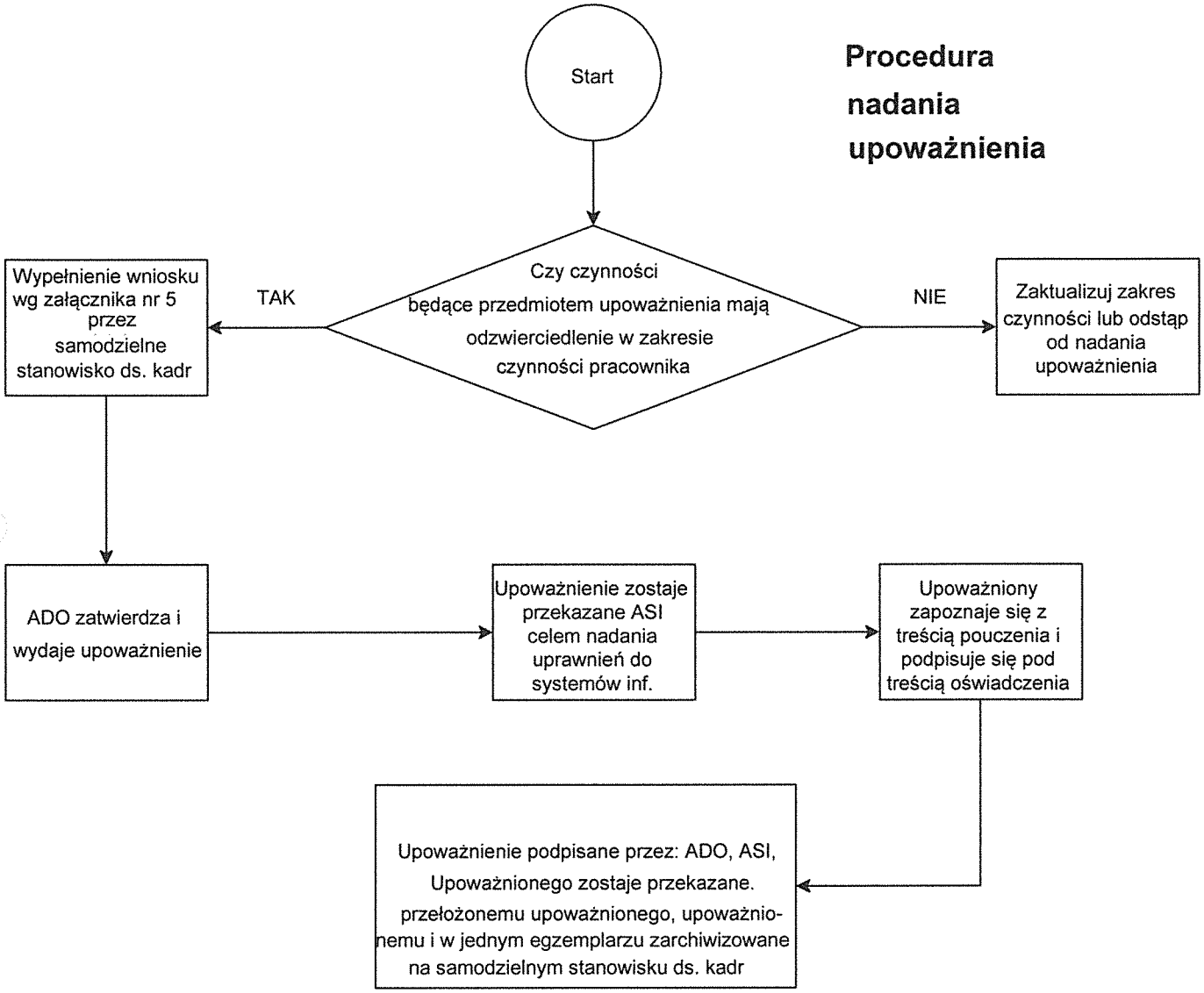
12. Jeżeli upoważnienie jest wydane dla kilku rodzajów czynności przetwarzania danych osobowych, okres 10 lat liczony jest od momentu zaprzestania realizowania ostatniego rodzaju czynności wymienionych we wniosku o nadanie upoważnienia.

13. Każdorazowa zmiana polegająca na dodaniu dodatkowych uprawnień użytkownikowi związanych z przetwarzaniem danych osobowych, wymaga powtórzenia całej procedury.

14. Zaprezentowana procedura ma zastosowanie również do osób fizycznych nieprowadzących działalności gospodarczej zatrudnionych w oparciu o umowę zlecenie, bądź dzieło, których zasady zawierania reguluje Kodeks cywilny.

Poniżej zaprezentowano schemat procesu nadawania upoważnienia.

Procedura nadania upoważnienia



2.2 Odebranie upoważnienia

Wydane upoważnienie do czynności przetwarzania danych osobowych może zostać odebrane w każdej chwili. Odebranie upoważnienia do przetwarzania danych osobowych mieści się wyłącznie w zakresie kompetencji kierownika jednostki. Odwołanie wydanego upoważnienia do przetwarzania danych osobowych może zaistnieć w następujących okolicznościach:

a) braku potrzeby dalszego wykonywania określonych czynności przetwarzania danych osobowych np.: na skutek zmiany zakresu czynności, zmiany stanowiska itp.,

b) wygaśnięcia bądź rozwiązania stosunku pracy przez pracownika,

c) wygaśnięcia lub zakończenia realizacji zawartej umowy cywilnej,

d) uzasadnione podejrzenie wobec osoby upoważnionej o braku zachowania należytej staranności przy procesie przetwarzania danych osobowych wynikającej z zasad określonych w *Polityce ochrony danych osobowych.*

Postępowanie:
1. Każda sytuacja zidentyfikowana jako spełniająca przesłanki wymienione w pkt. od a) do d) stanowi bezpośrednią implikację do podjęcia działań związanych z odebraniem nadanego wcześniej upoważnienia.

2. Samodzielne stanowisko ds. kadr jako osoba nadzorująca proces fluktuacji kadr i określania indywidualnych zakresów obowiązków, przygotowuje wniosek o odwołanie upoważnienia do przetwarzania danych osobowych w 3 egzemplarzach wg załącznika nr 6 do *Polityki ochrony danych osobowych,* w sytuacji:

a) zmiany stanowiska przez upoważnionego użytkownika,

b) w związku ze zmianą zakresu czynności upoważnionego użytkownika, zgłoszoną przez jego bezpośredniego przełożonego,

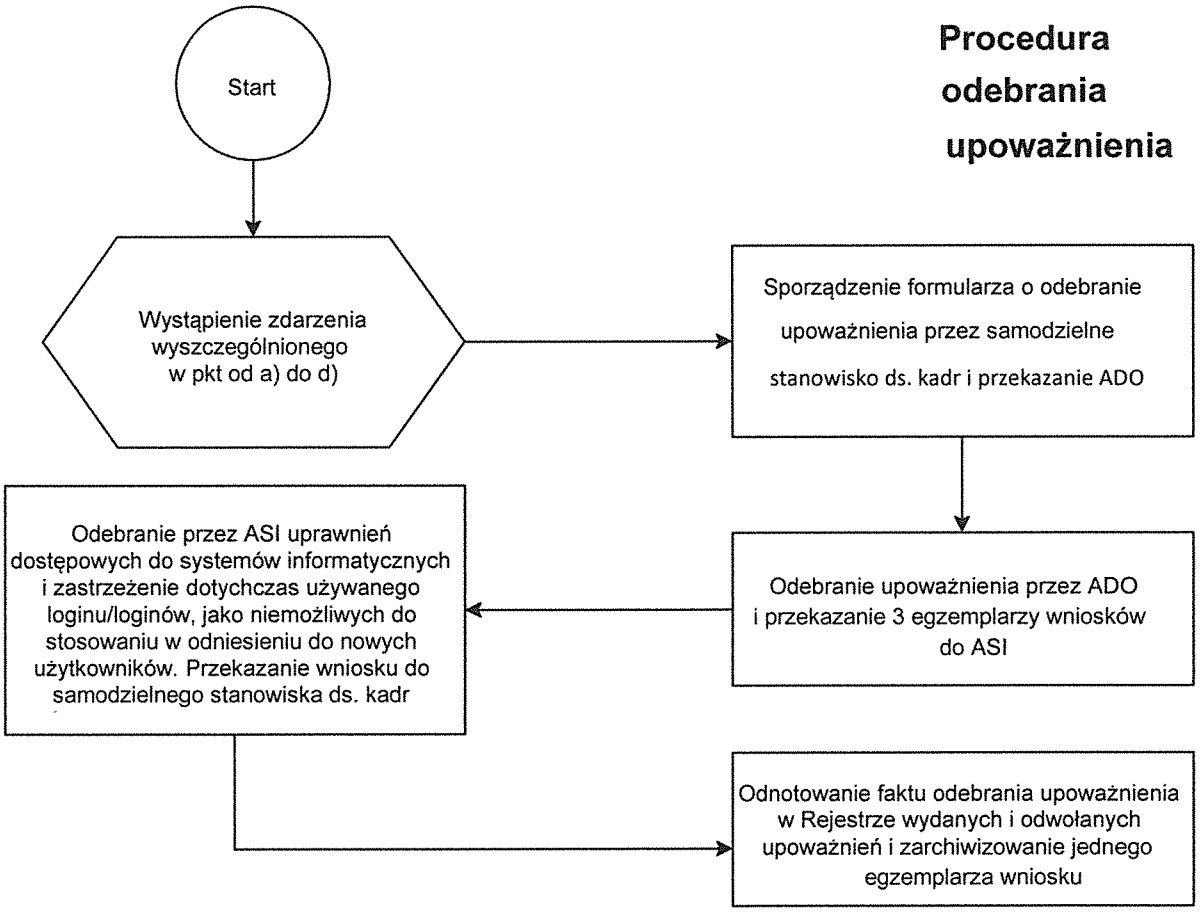
a) wygaśnięcia stosunku pracy upoważnionego użytkownika, niezależnie od powodów ustania zatrudnienia,

3. ADO lub osoba przez niego umocowana, dokonuje czynności odebrania upoważnienia potwierdzając ten fakt na wszystkich 3 egzemplarzach wniosku o odwołanie przedłożonych przez samodzielne stanowisko ds. kadr.

4. Następnie formularze odwołania upoważnienia trafiają do ASI, a ten w stosunku do użytkownika, któremu odbierane są określone upoważnienia, odbiera prawa dostępowe do właściwych systemów informatycznych. Należy podkreślić, że wcześniej przypisane użytkownikowi loginy, które w momencie cofnięcia posiadanych uprawnień dostępowych przestają być aktywny, nie mogą nigdy w przyszłości zostać nadany kolejnemu, nowemu użytkownikowi.

5. Po zakończeniu procedury przez ASI, potwierdzone przez niego odwołanie upoważnienia (3 egzemplarze) przekazuje do samodzielnego stanowiska ds. kadr. Rozdzielnik wniosków o odebranie nadanych upoważnień jest analogiczny jak w przypadku wniosku o ich nadanie.

Poniżej zaprezentowano schemat postępowania przy realizacji wniosku o odebranie upoważnienia.



3. Procedura reakcji na ujawnione naruszenie

Zgodnie z przyjętą w Polityce ochrony danych osobowych definicją, przez naruszenie ochrony danych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

a) zniszczenia (utrata atrybutu dostępności),

b) utracenia (utrata atrybutu dostępności i integralności),

c) zmodyfikowania (utrata atrybutu integralności),

d) nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (utrata atrybutu poufności).

Postępowanie:

W przypadku wystąpienia jakiegokolwiek zdarzenia, zjawiska, które będzie charakteryzowało się znamionami określonymi w pkt od a) do d), należy wszcząć procedurę reakcji na ujawnione naruszenie.

1. Ujawnienia naruszenia przetwarzania danych osobowych może dokonać każdy, niezależnie od faktu, czy jest pracownikiem, klientem jednostki lub w żaden sposób nie musi być powiązany z jednostką. Ujawnienie naruszenia mogą również dokonać media.

2. Za moment ujawnienia naruszenia uważa się czas, w którym ktokolwiek z wymienionych tj. pracownik administratora, administrator, inspektor ochrony danych powziął informacje o wystąpieniu naruszenia lub informacja taka został opublikowana w mediach. Nie ma znaczenia sposób powzięcia informacji np. zgłoszenie mailowo, telefonicznie, osobiste stwierdzenie naruszenia, komunikat prasowy itd.

3. Należy pamiętać, iż od momentu powzięcia informacji o naruszeniu w terminie 72 h, należy powiadomić organ nadzorczy o jego wystąpieniu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.

4. Ktokolwiek będąc pracownikiem jednostki powziąwszy informacje o naruszeniu ochrony danych osobowych, winien dokonać natychmiastowej oceny, czy swoim działaniem może ograniczyć naruszenie lub je powstrzymać (np. zdejmując z tablicy ogłoszeń zamieszczony wykaz zawierający dane osobowe, wyłączając jednostkę komputerową, na której doszło do nieupoważnionego dostępu do danych, odebrania dokumentacji zawierającej dane osobowe od osób, które przypadkowo weszły w jej posiadanie - znalazły itp. działania).

5. W przypadku braku możliwości ograniczenia lub powstrzymania naruszenia osoba, która powzięła o tym fakcie wiedzę, jest zobowiązana do powiadomienia administratora danych osobowych oraz inspektora ochrony danych.

6. Administrator wspólnie z IOD, wykorzystując wszelkie dostępne im środki, podejmują działania mające na celu wyeliminowanie zjawiska naruszenia lub jego maksymalne ograniczenie.

7. IOD dokonuje ustaleń mających na celu:

- zidentyfikowanie przyczyny naruszenia,

- określenie kategorii i liczby osób, których prawa i wolności mogą ucierpieć w efekcie naruszenia,

- oszacowanie możliwych do zastosowania środków w celu zminimalizowania negatywnych skutków naruszenia w stosunku do właścicieli danych osobowych.

Z dokonanych ustaleń IOD sporządza protokół i przedkłada go do zatwierdzenia administratorowi.

8. Administrator wspólnie z IOD dokonują analizy ryzyka stopnia naruszenia praw i wolności właścicieli danych osobowych w stosunku, do których doszło do naruszenia danych.

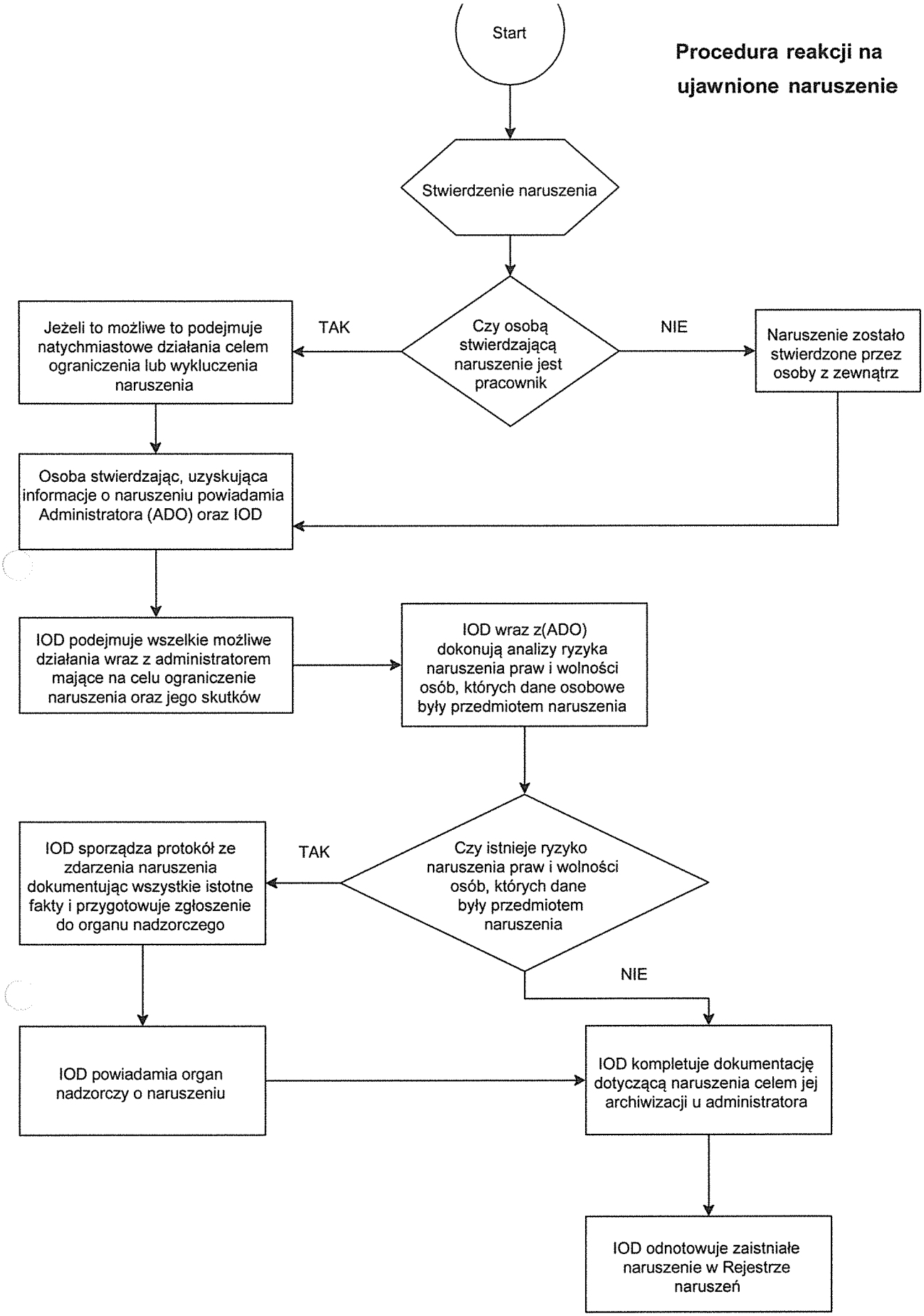
9. Na podstawie wyników przeprowadzonej analizy, o której mowa w pkt. 8 administrator w porozumieniu z IOD podejmuje decyzję o zgłoszeniu naruszenia organowi nadzorczemu lub braku wystarczających przesłanek do jego powiadamiania o naruszeniu.

10. Jeżeli istnieje taka konieczność IOD powiadamia organ nadzorczy o wystąpieniu naruszenia.

11. W przypadku, jeżeli naruszenie ma wpływ na prawa i wolności osób fizycznych należy podjąć działania związane z poinformowaniem tych osób o wystąpieniu naruszenia w stosunku do dotyczących ich danych osobowych i w razie konieczności poinformować o działaniach, które mogą podjąć, by chronić się przed konsekwencjami naruszenia.

12. IOD kompletuje dokumentację dotyczącą naruszenia i zgłoszenia do organu nadzorczego oraz odnotowuje jego wystąpienie w *Rejestrze naruszeń* stanowiącym załącznik nr 2 do niniejszego dokumentu.

Procedura reakcji na ujawnione naruszenie



4. Procedura udostępniania danych osobowych

Możliwe jest ujawnienie danych osobowych (udostępnienie), bez jakiejkolwiek umowy powierzenia danych do dalszego przetwarzania kategorii odbiorców tj.: organom publicznym, które mogą wykorzystywać dane wyłącznie dla potrzeb sprawowanych funkcji publicznych i są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym, zgodnie z obowiązującym prawem. Ponieważ prawo do ochrony danych osobowych nie jest prawem bezwzględnym, przetwarzane dane możemy ujawnić (udostępnić) następującym organom:

a) podatkowym,
b) celnym,
c) policji, prokuraturze, sądom,
d) Straży Granicznej,
e) CBA, CBŚ, ABW

Żądanie ujawnienia danych osobowych, z którymi występują takie organy publiczne, powinno mieć zawsze formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych.

Postępowanie:

1. Jeżeli do jednostki wpłynie wniosek o ujawnienie „udostępnienie" danych osobowych w odniesieniu do osoby / osób, które zostały w jakiś sposób we wniosku określone z jednoczesnym wskazaniem kategorii danych mających być przedmiotem ujawnienia i wniosek ten złoży organ zawarty w katalogu od lit. a) do lit. e), to jednostka jest zobowiązana do ujawnienia danych będących przedmiotem wniosku.

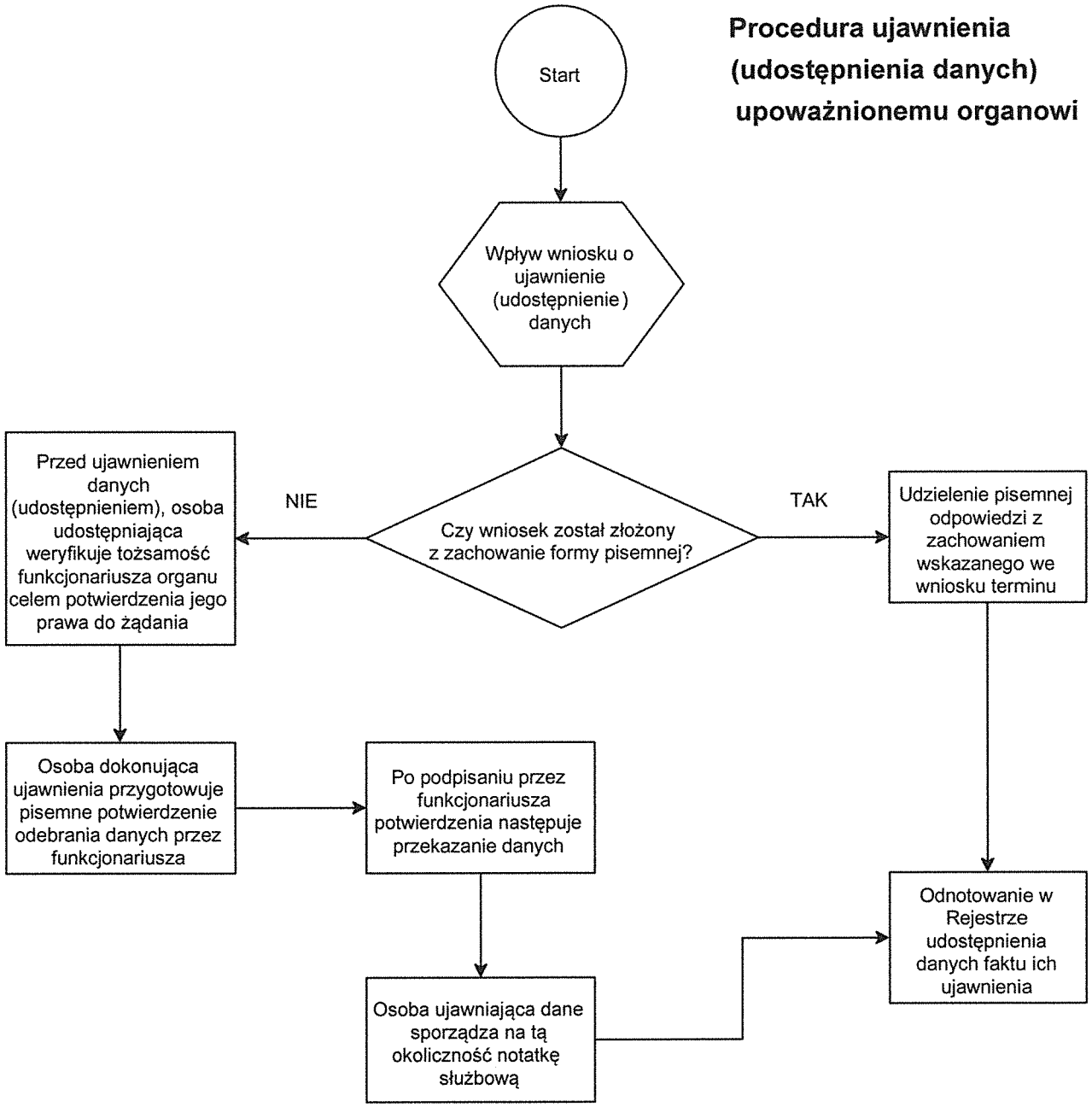
2. Co do zasady wniosek taki winien mieć formę pisemną i wskazywać precyzyjnie organ żądający ujawnienia oraz podstawę prawną, sankcjonującą takie żądanie. Dopuszcza się sytuacje związane z ujawnieniem danych osobowych w związku z ustnym żądaniem funkcjonariusza publicznego, zatrudnionego przez organ w przypadku stanu wyższej konieczności (np. pościg za przestępcą, ratowanie życia ludzkiego lub mienia).

3. Każde ujawnienie (udostępnienie) danych, musi zostać zaewidencjonowane w *Rejestrze udostępnienia danych osobowych* prowadzonym przez ADO. Wzór rejestru stanowi załącznik nr 3 do niniejszego dokumentu.

4. W przypadku ujawnienia (udostępnienia) danych osobowych, na skutek ustnego żądania funkcjonariusza publicznego zatrudnionego w organie, których katalog został określony we wstępie, osoba ujawniająca żąda pisemnego potwierdzenia przekazania danych od funkcjonariusza, któremu dane są przekazywane.

5. Potwierdzenie powinno zawierać następujące informacje:
- miejsce i datę ujawnienia (udostępnienia) danych osobowych,
- precyzyjne określenie organu wraz ze wskazaniem jego siedziby,
- imię i nazwisko oraz stopień funkcjonariusza lub inne dane zawarte w posiadanej przez niego legitymacji służbowej, umożliwiające jego jednoznaczną identyfikację,
- określenie kategorii osób, których dane były przedmiotem ujawnienia, wraz ze wskazaniem kategorii ujawnionych danych.

6. W przypadku ujawnienia (udostępnienia) danych na ustne żądanie funkcjonariusza uprawnionego organu, osoba dokonująca ujawnienia (udostępnienia), sporządza notatkę służbową opisującą przebieg zdarzenia.



Załączniki:

Załącznik nr 1 – Wzór zgody na przetwarzanie danych osobowych

Załącznik nr 2 – Rejestr naruszeń

Załącznik nr 3 – Rejestr udostępnienia danych osobowych

Zgoda na przetwarzanie danych osobowych

Ja ..... niżej podpisana/y,
(imię i nazwisko upoważniającego)

wyrażam wyraźną i dobrowolną zgodę na przetwarzanie przez Urząd Miejski w Łobzie nw. kategorii moich danych osobowych tj.

1. .....
(kategoria danych)

2. .....
(kategoria danych)

3. .....
(kategoria danych)

w zakresie niezbędnym dla realizacji nw. celu/celów*. Jednocześnie oświadczam, że zapytanie o zgodę zostało mi przedstawione w wyraźnej i zrozumiałej dla mnie formie i zrozumiałam(em) treść udzielonej mi informacji odnoszącej się do przetwarzania moich danych osobowych.

1. .....

.....
Data i czytelny podpis osoby wyrażającej zgodę

2. .....

.....
Data i czytelny podpis osoby wyrażającej zgodę

3. .....

.....
Data i czytelny podpis osoby wyrażającej zgodę

Uwaga! *Przetwarzanie danych dla różnych celów wymaga odrębnej zgody dla każdego z celów. W przypadku jednoczesnego pozyskiwania danych dla różnych celów, wszystkie cele przetwarzania należy określić w informacji dla osoby wyrażającej zgodę.*

**niepotrzebne skreślić*

Informacja dla osoby wyrażającej zgodę

Administratorem Pani/Pana/dziecka danych osobowych jest:
Burmistrz Łobza z siedzibą: ul. Niepodległości 13, 73-150 Łobez. Z administratorem danych można się skontaktować poprzez adres e-mail: lobez@lobez.pl lub telefonicznie pod numerem 91 39 740 01/02 lub pisemnie na adres siedziby administratora.

Inspektor ochrony danych.
Administrator wyznaczył inspektora ochrony danych osobowych, z którym może się Pani/Pan* skontaktować poprzez email: iod@lobez.pl lub pisemnie na adres siedziby administratora. Z inspektorem ochrony danych można się kontaktować, w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.

Cele i podstawy przetwarzania.
Podane przez Panią/Pana* dane osobowe będą przetwarzane dla celów:.....

.....

Podane dane są przetwarzane na podstawie art.6 ust. 1 lit. a *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych „RODO")*, (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), czyli Pani/Pana* zgody

Odbiorcy danych osobowych.
Odbiorcami danych osobowych będą: .....

.....

jednostki administracji publicznej uprawnione do sprawowania kontroli i nadzoru nad prawidłowością funkcjonowania administratora oraz jednostki i organy administracji publicznej mogące potwierdzić prawdziwość podanych przez Panią/Pana* informacji.

Okres przechowywania danych.
Dane będą przechowywane przez okres ..... lat poczynając od 1 stycznia roku następnego po roku, w którym nastąpiło wyrażenie zgody.

Sposób przetwarzania danych osobowych
Pani/Pana* dane nie będą/ będą* przetwarzane w sposób zautomatyzowany oraz zostaną poddane/ nie zostaną poddane* profilowaniu.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Pani/Panu*:

a) prawo dostępu do swoich danych oraz otrzymania ich kopi,
b) prawo do sprostowania (poprawiania) swoich danych,
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej,
d) prawo do ograniczenia przetwarzania danych,
e) prawo do wycofania zgody
f) prawo do wniesienia skargi do Prezesa UODO na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa.

Informacja o wymogu podania danych.
Podanie przez Panią/Pana* danych jest dobrowolne, jednakże odmowa ich podania uniemożliwi .....

*niepotrzebne skreślić

Rejestr naruszeń danych osobowych

Lp.	Opis naruszenia ze wskazaniem daty powstania i jego ujawnienia	Przyczyny naruszenia	Przebieg naruszenia	Kategorie osób oraz kategorie danych będące przedmiotem naruszenia	Zgłoszono / nie zgłoszono do UODO naruszenia. Powody niezgłoszenia

Rejestr udostępnienia danych osobowych

Lp.	Wskazanie daty udostępnienia oraz organu, któremu dane zostały udostępnione	Forma żądania udostępnienia pisemny wniosek/ustne żądanie	Wskazanie osoby udostępniającej oraz osoby odbierającej dane osobowe	Kategorie osób których dane były przedmiotem udostępnienia	Kategorie udostępnionych danych osobowych